Safeguarding Client Information*

- **Only ask for and share the minimum amount of client information that is necessary to do your job.**

- **Always identify yourself by wearing a County ID. Ensure that visitors are wearing badges.**

- **Immediately report any lost or stolen client information or unauthorized disclosures of client information.**

- **Make sure that on-site contractors, temps, and volunteers complete all required trainings and follow department policies and procedures.**

- **Protect conversations**
  - ➢ If possible, use a private interview room to meet with a client. Keep voices down if you must talk with a client in an open area.
  - ➢ Do not discuss clients in common areas such as an elevator or in a hallway.
  - ➢ Never leave confidential information on a client's voicemail, unless the client has given you permission.

- **Protect written information**
  - ➢ Store client records in a secure location away from public areas.
  - ➢ Never leave client information in plain view of others. Keep identifying information (e.g. names, addresses) concealed when walking in public areas.
  - ➢ Never leave client records or notes unattended at your workstation. Lock your office, or place the records in a locked cabinet or desk, even if you are leaving for a brief time period.
  - ➢ When disposing of documents that contain client identifying information, be sure to shred them.
  - ➢ Do not place copy machines, fax machines, printers, incoming or outgoing mail and staff mailboxes in locations that are accessible to the public.
  - ➢ Promptly remove client information from copy, print and fax machines.
  - ➢ Follow the procedures on the back of this sheet for faxing client information.

- **Protect electronic information**
  - ➢ Never share your computer access password with anyone, or post your password where others can see it.
  - ➢ Never save client information to a shared drive or your computer's local drive.
  - ➢ Do not save client information to a portable computer device (e.g. laptop, Blackberry) or to removable media (e.g. floppy discs, compact discs, flash memory cards) unless HHS has issued the device to you and has given you permission. See Permission Form attached to the policy*.
  - ➢ Do not save client information to your home computer.
  - ➢ Never send client information in the subject line or body of an email. Follow the email procedures on the back of this sheet.

- **Working with client information when away from the office**
  As a general rule, client information may not be removed from the worksite. Staff who have a legitimate need to remove client information to do their jobs must obtain written permission to do so from their supervisors and service chiefs, and must agree to follow specific safeguards to protect the information. See Permission Form attached to the policy*.

- **Questions?**
  Contact your service area HIPAA Coordinator, or Debra Rosenberg, HIPAA Program Manager at 240 777-3819.

***A full version of the HHS Safeguarding Policy and Procedures can be accessed via the HHS Intranet at http://portal.mcgov.org/hhs/hipaa/.**

Emailing Client Information

1. Never put client information in the subject line or body of an email. If you need to send client information via email, always put the client information in a password protected attachment.

2. Verify that you have the recipient's correct email address.

3. To password protect an attachment follow these instructions: In Word and Excel, click on *Tools, Options, Security* and then enter the password that will be required to open the document after it is saved. Do not include the password in your Email to the recipient! Call the recipient to tell them the password to open the attachment. If the recipient is someone who you regularly work with (e.g. co-workers within an HHS program) you can make this process less burdensome by agreeing to a password ahead of time, and then changing the password at regular intervals.

4. A confidentiality notice like the one written below should be included in the body of your email. You should add a notice like this to your signature so that it goes out with all emails. For instructions on how to add a notice to your signature, go to Outlook and type in the help box "create a signature for messages".

   CONFIDENTIALITY NOTICE: This email message, including any attachments, is for the sole use of the intended recipient(s). The information contained in this message may be confidential. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message. Thank you

5. When forwarding or replying to an email, be sure that there is no client information in the subject line or body of the email.

6. These procedures apply to **all** email transmissions, i.e. emails that are sent **outside** of the County network, and emails that are sent to an HHS or County employee **within** our network.

Sending or Receiving Client Information by Fax

1. Check the fax number to be sure it is correct and let the recipient know that the fax is on its way.

2. Attach a cover sheet that includes a confidentiality notice as follows:

   CONFIDENTIALITY NOTICE: This transmission may contain confidential information. If you are not the intended recipient, any review, use, disclosure or distribution of the contents of this transmission is prohibited. If you have received this transmission in error, please immediately notify the sender by telephone and destroy any copies of this material. Thank you.

3. After you have sent the fax, check the confirmation sheet to verify that the fax was sent to the correct number.

4. File the confirmation sheet along with the document in the case record.

5. When receiving a Fax with client information, retrieve the fax immediately.